UCSM에서 서드파티 인증서 생성 및 사용

목차

소개

이 문서에서는 보안 통신을 위해 UCS(Unified Computing System)에서 서드파티 인증서를 생성하고 사용하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CA 권한 액세스
- UCSM 3.1

사용되는 구성 요소

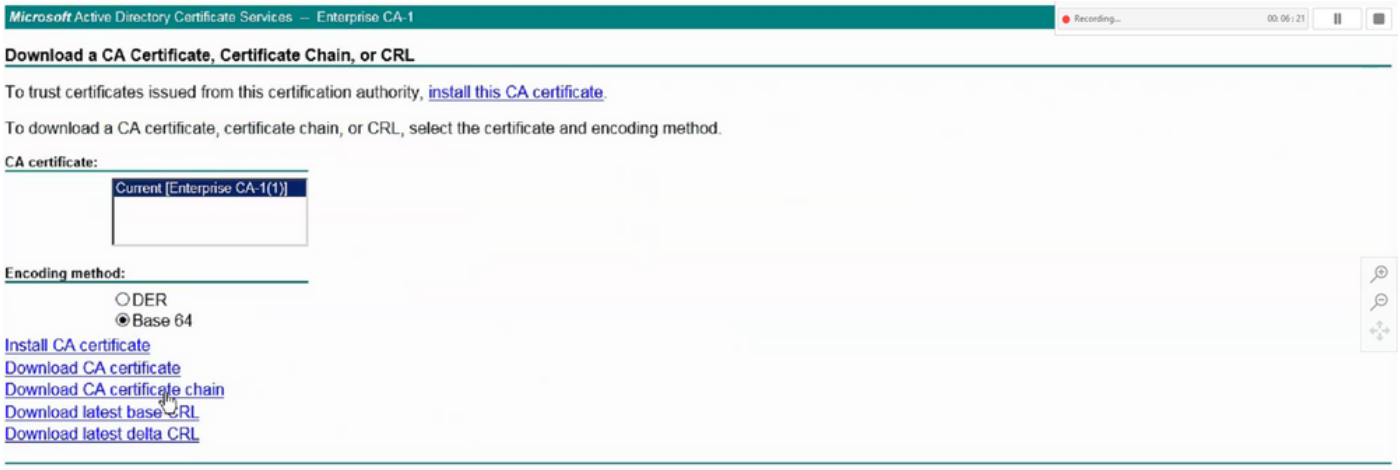
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성 단계

신뢰 지점 구성

1단계

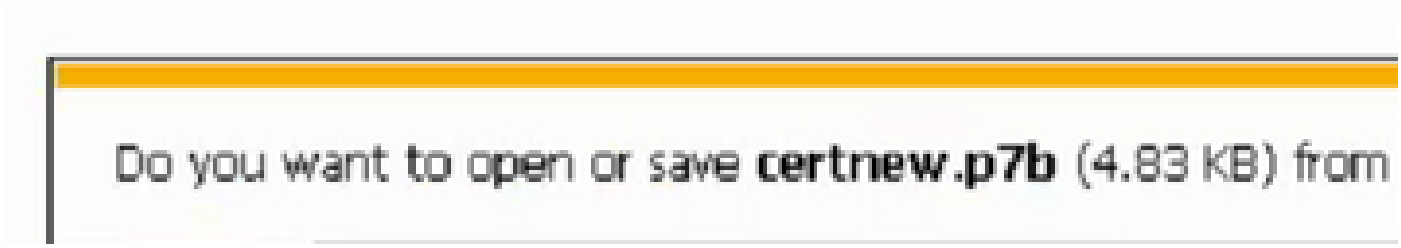
- CA 기관에서 인증서 체인을 다운로드하여 Trust-Point를 생성합니다. 인증서 서버에서 http://localhost/certsrv/Default.asp를 참조하십시오.
- 인코딩이 Base 64로 설정되어 있는지 확인합니다.



CA 기관에서 인증서 체인 다운로드

2단계

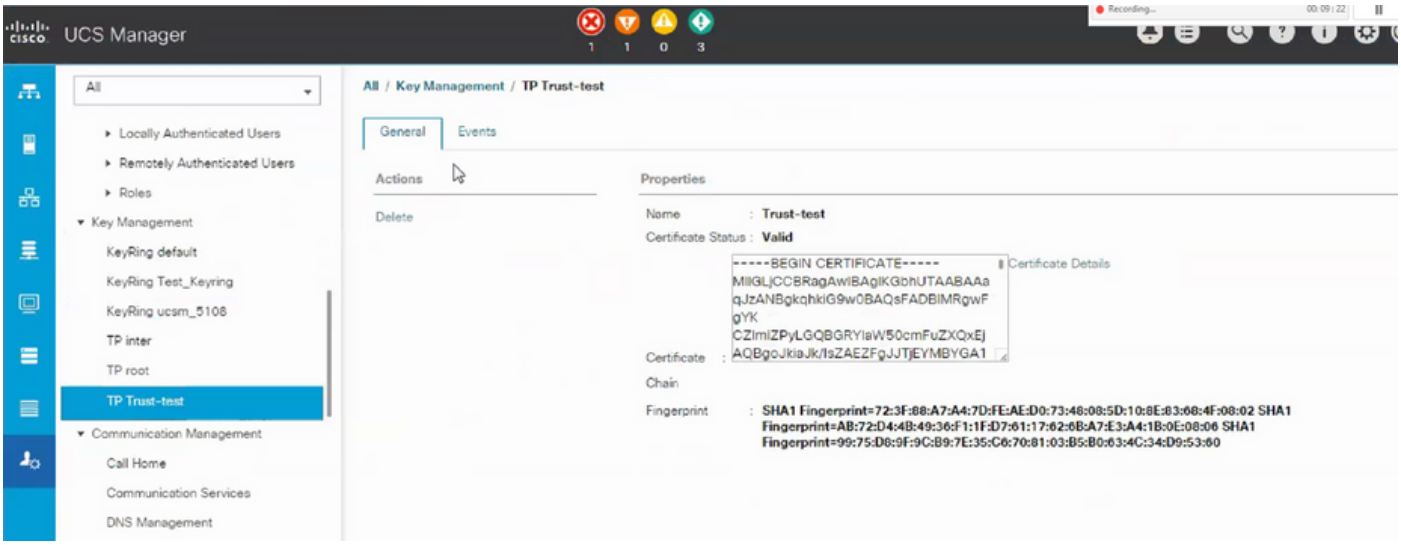
- 다운로드한 인증서 체인은 PB7 형식입니다.



- OpenSSL 도구를 사용하여 .pb7 파일을 PEM 형식으로 변환합니다.
- 예를 들어 Linux에서는 터미널에서 이 명령을 실행하여 변환- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem을 수행할 수 있습니다.

3단계

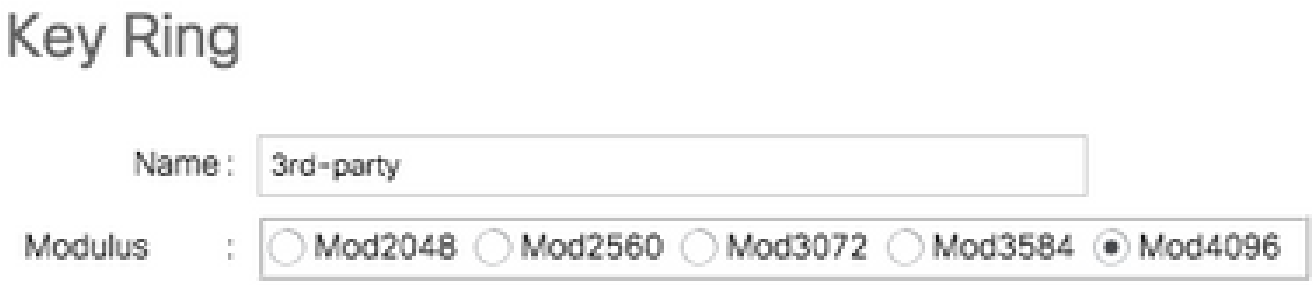
- UCSM에서 Trust-Point를 생성합니다.
- Admin(관리) > Key Management(키 관리) > Trustpoint(신뢰 지점)로 이동합니다.
- Trust-point를 만들 때 이 섹션의 2단계에서 만든 .PEM 파일의 전체 내용을 인증서 세부 정보 공간에 붙여넣습니다.



키 및 CSR 생성

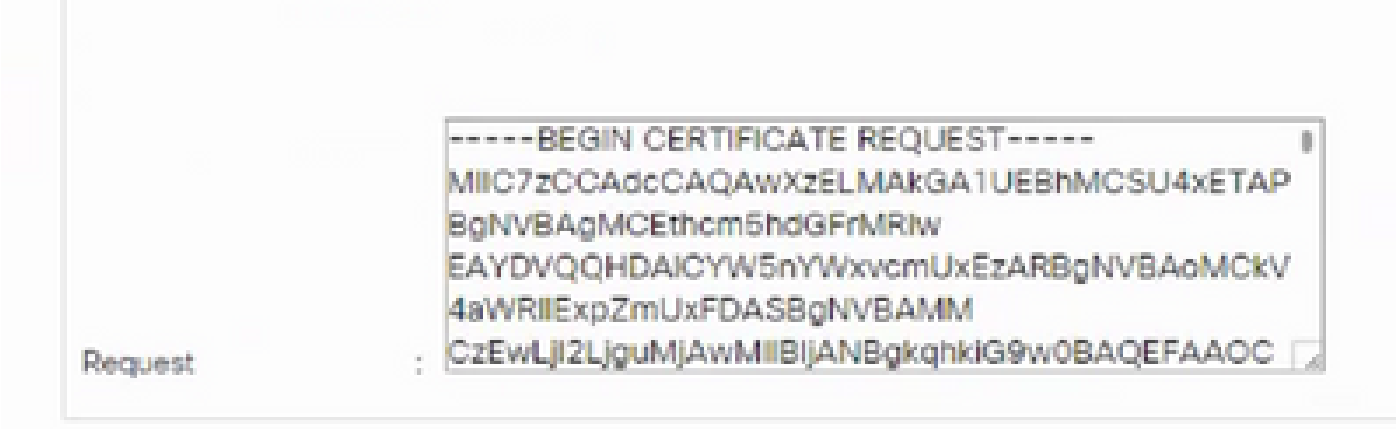
1단계

- UCSM > Admin > Key Management > Keyring으로 이동합니다.
- 서드파티 인증서에 필요한 모듈러스를 선택합니다.



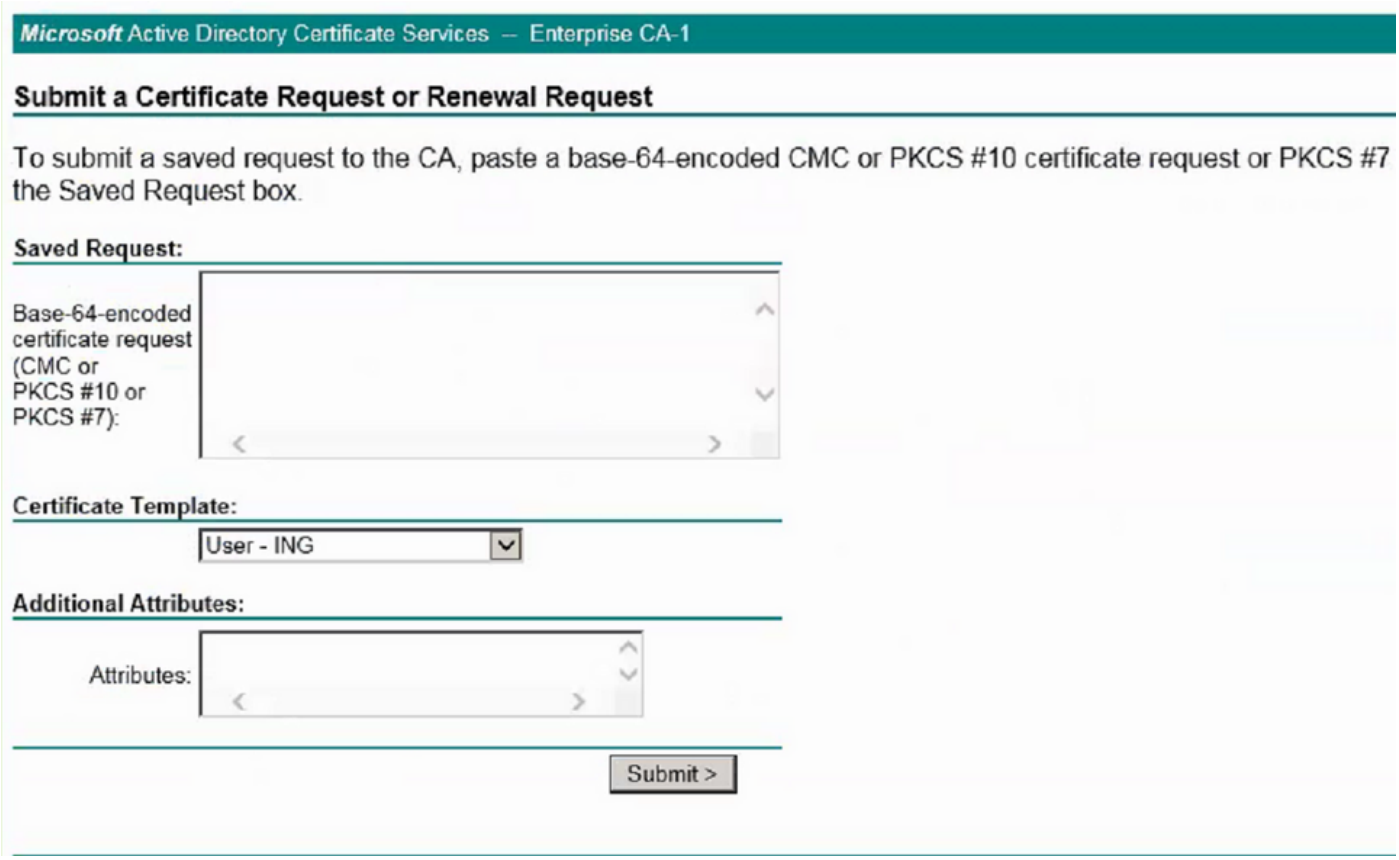
2단계

- 인증서 요청 생성을 클릭하고 요청된 세부 정보를 입력합니다.
- 요청 필드의 내용을 복사합니다.



3단계

인증서를 생성하려면 아래 표시된 공간에 단계 2의 복사된 요청을 붙여넣습니다.



4단계

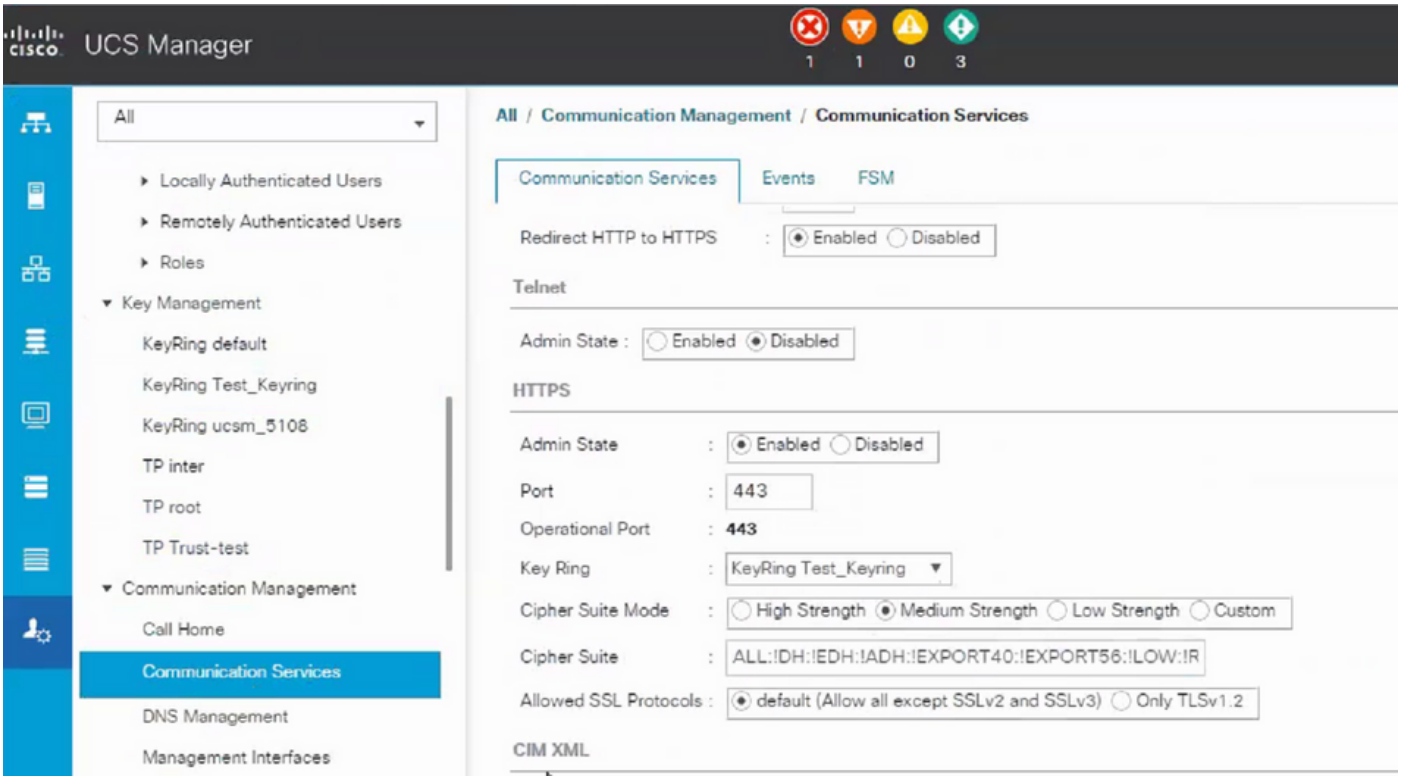
- 제출되면 새 인증서가 생성됩니다. 파일을 열고 새로 생성된 인증서의 모든 내용을 이 섹션의 1단계에서 생성한 키링의 인증서 필드에 복사합니다.

- Create Keyring and CSR(키 및 CSR 생성)의 3단계에서 생성한 드롭다운에서 신뢰 지점을 선택합니다.

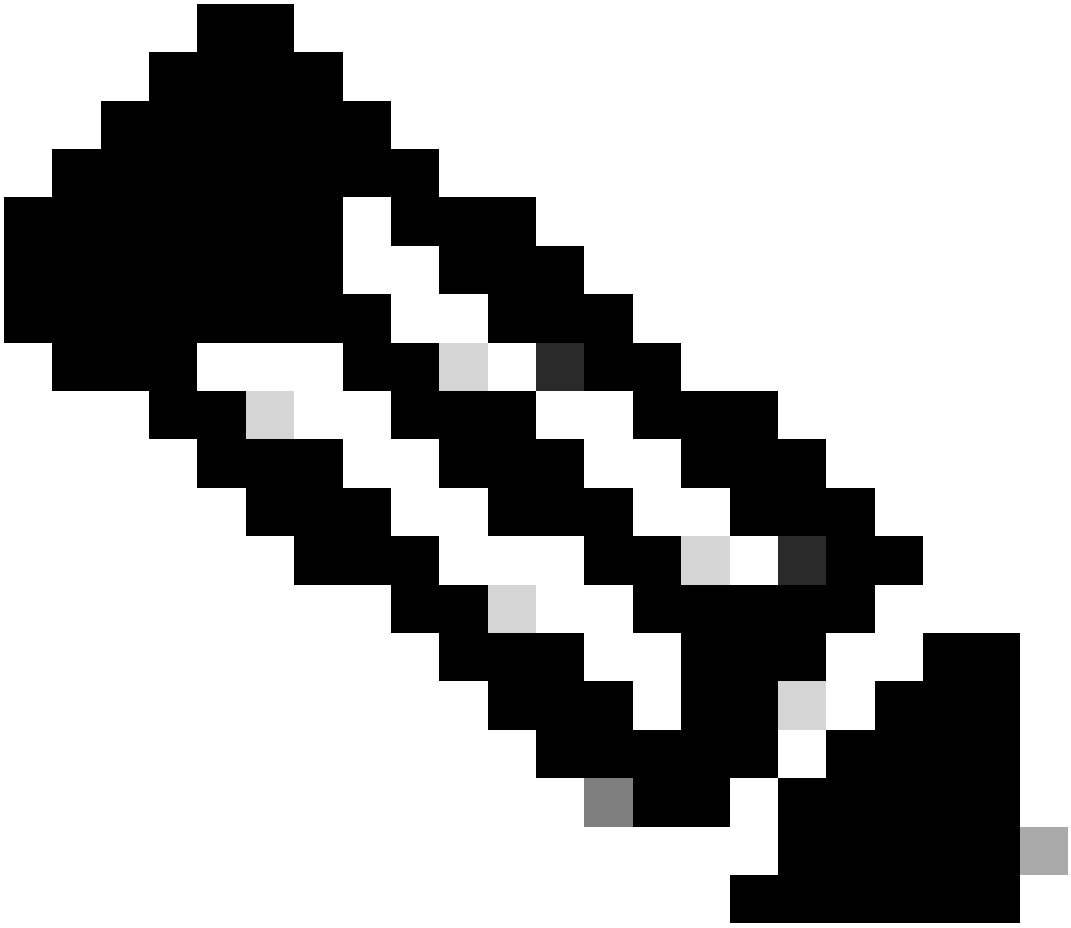
키링 적용

1단계

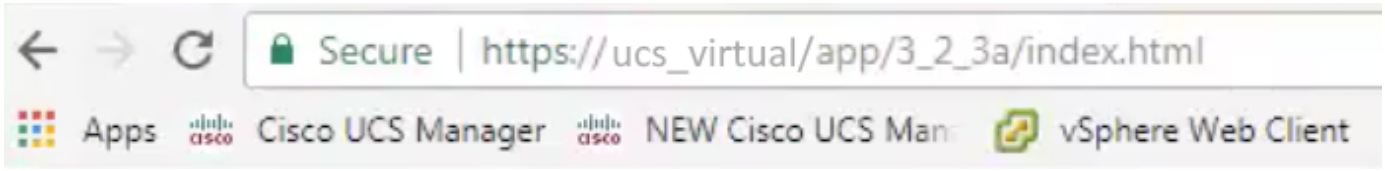
아래 표시된 대로 통신 서비스에서 생성된 키를 선택합니다.



키링을 변경하면 UCSM에 대한 HTTPS 연결이 웹 브라우저에 보안 상태로 표시됩니다.



참고: 이렇게 하려면 로컬 데스크톱에서 UCSM과 동일한 CA 기관의 인증서를 사용해야 합니다.



관련 정보

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.